Restoring balance between stakeholders - problems, tools and proof of concept

Kresimir Kalafatic
kresimir.kalafatic@gmail.com

***Abstract*—In every process there are multiple stakeholders involved. The interest of all stakeholders are not the same. The stakeholders who have direct control of the process and infrastructure have advantage over the stakeholders who have interest in the process, but not direct control. This paper will describe the problems, tools and proof of concept for restoring balance between the stakeholders.**

***Index Terms*—security of stakeholders, blockchain, supply chain of documentation, legal documents and papers**

I. Introduction

Today most software providers on their software download page publish link to digitally signed application with SHA256 digest of signed application. This information increases security of the application supply chain to the user, but also implies that the application without the digital signature and published digest is not to be trusted by the user.

Today most of the documentation, research papers and legislation is available in PDF format, and even though the PDF format supports digital signing for two decades, digital signature of the PDF document is rarely used. Only security feature for this critical information is TLS encryption between server and user computer.

II. Problems - Questions for readers thoughts

How can peers in peer review be sure they reviewed and approved the same document if they didn't compare the SHA256 digest of the documents received, reviewed and published?

How can citizen or company prove that the document downloaded from official pages of legislator, regulator or company where changed by hackers on the official site? Currently only by getting public notification that the official site has been hacked.

III. Tools

Tools needed for implementation:

1) latex or other document format able to create PDF
2) SHA256 digest calculation tool
3) PDF document signing tool
4) digital certificate for digital signature
5) web page for download

IV. Procedure

The implementation procedure:

1) write the document and references with tool 1)
2) generate SHA256 digest of the referenced documents using tool 2) and add them to reference text
3) generate PDF output in tool 1)
4) digitally sign the PDF with tool 3) using certificate 4)
5) generate SHA256 digest of the produced documents using tool 2)
6) publish document and SHA256 digest of the signed document on the download page

V. Security elements

The mentioned concept has following security elements embedded in it:

- document is digitally signed preventing data altering
- published SHA256 digest on the download page, protects user from opening a malicious documentation
- the reference with SHA256 digest of documentation is proof of previous work and creates blockchain of directly or indirectly referenced documents
- the reference with SHA256 digest enables readers for quick finding of the relevant and trustworthy referenced documentation
- the document provider is protected from publishing falsified documents under the providers name or logo
- the digital signature of the produced PDF document identifies the author and contact information

VI. Proof of concept

This paper is written in the described procedure. It explains some principles from previous papers and digitally signs the SHA256 digest of previous papers. This is a seventh block in this blockchain.

VII. Conclusion

Paper banknote are a legal tender, provide direct ownership of central bank money and secures the banknote holder in the case infrastructure of bank is not available. Technical concepts described and proved on this one page enable direct copy ownership of digital document and proof of document authenticity and integrity. It promotes inclusion of stakeholders in the process and restoration of some balance between stakeholders.

References

[1] K.Kalafatic, "When all efforts fail, you go back to basics", SHA256:af0d5f34a5c5bca131e3c6ca83614ca188187176af61843e033f336861a03a3e.

Disclaimer: The views and opinions expressed in this paper are those of the author and do not necessarily reflect the official policy or position of the company, legislator, regulator or any other organization. User/Reader should consult local regulation, legislation and contracts for usage.